

ON THE GROUP OF SEPARABLE QUADRATIC ALGEBRAS AND STACKS

ILIA PIRASHVILI

ABSTRACT. The aim of this paper is to study the group of isomorphism classes of torsors of finite flat group schemes of rank 2 over a commutative ring R . This, in particular, generalises the group of quadratic algebras (free or projective), which is especially well studied. Our approach however, yields new results even in this case.

1. INTRODUCTION

We are going to study the group of separable quadratic algebras, which was introduced by Bass in [1, Section 4.3] and was extensively studied by several authors (see for example [7], [4] and references therein), using the methods of 2-dimensional categorical algebra. Our methods are based on the fact that stackification is an exact 2-functor.

Let R be a commutative ring and we denote by $\mathrm{Qu}(R)$ the group of isomorphism classes of separable quadratic R -algebras [4, Ch. 12] and by $\mathrm{Dis}(R)$ the group of isomorphism classes of nonsingular symmetric bilinear R -modules, which are finitely generated and projective of rank 1 [4, Ch. 4C]. According to [4, Statement 12.6, p.178], one has an exact sequence of abelian groups

$$\mathrm{Qu}(R) \rightarrow \mathrm{Dis}(R) \rightarrow \mathrm{Dis}(R/4R).$$

Our goal is to extend this important exact sequence on the left hand side. It follows from our results that the following is true:

Theorem 1.1. *If 2 is not a zero-divisor in R , one has an exact sequence of abelian groups*

$$0 \rightarrow \mathbb{Z}_2(R) \rightarrow \mu_2(R) \rightarrow \mathrm{Im}(\mu_2(R/4R) \rightarrow \mu_2(R/2R)) \rightarrow \mathrm{Qu}(R) \rightarrow \mathrm{Dis}(R) \rightarrow \mathrm{Dis}(R/4R).$$

Here

$$\mu_2(R) = \{r \in R \mid r^2 = 1\} \text{ and } \mathbb{Z}_2(R) = \{r \in R \mid r^2 = r\}.$$

The operation in \mathbb{Z}_2 is given by $r +_1 s = r + s - 2rs$ (see [4, p. 202]). The first nontrivial map is given by $r \mapsto 1 - 2r$.

In order to obtain the above, we are going to define a symmetric categorical group $\mathfrak{Qu}(R)$ such that the groups $\mathrm{Qu}(R)$ and $\mathbb{Z}_2(R)$ are its π_0 and π_1 respectively (see Section 2 for symmetric categorical groups). Similarly, behind of the groups $\mathrm{Dis}(R)$ and $\mu_2(R)$ there is a symmetric categorical group $\mathfrak{Dis}(R)$, while the groups $\mathrm{Dis}(R/4R)$ and $\mathrm{Im}(\mu_2(R/4R) \rightarrow \mu_2(R/2R))$ are obtained from the symmetric categorical group $\mathfrak{Dis}^{-2,1}(R)$. Hence, it suffices to show that $\mathfrak{Qu}(R)$, $\mathfrak{Dis}(R)$ and $\mathfrak{Dis}^{-2,1}(R)$ fit in an exact sequence of symmetric categorical groups, and then apply the classical six-term exact sequence [3, p.84] involving π_i , $i = 0, 1$. The symmetric categorical groups $\mathfrak{Qu}(R)$ and $\mathfrak{Dis}(R)$ are classical and they appear (at least implicitly) in many papers, for example in [4]. However, $\mathfrak{Dis}^{-2,1}(R)$ is new. The next observation is that, by varying R , these symmetric categorical groups form stacks in the Zariski topology.

As it turns out, they can be seen as the stackifications of the analogue prestacks of symmetric categorical groups, based on free modules instated of projective ones. It is a fairly easy exercise to show that the 'free' versions of the above symmetric categorical groups fit in an exact sequence. Since stackification sends exact sequences to exact ones, the result then follows.

Actually, we will work in a more general setting than that of separable quadratic algebras. In fact, we will fix a commutative and cocommutative Hopf algebra J , which is free of rank 2 as an R -module. It is a classical fact that any such Hopf algebra is uniquely determined by a pair

(p, q) of elements of R , such that $pq + 2 = 0$ (see [5, Theorem 1.2]). Our main object of interest will be the group $\text{Qu}^{pq}(R)$ of J -Galois algebras, with our main result being Theorem 4.8. Since $\text{Qu}(R) = \text{Qu}^{-2,1}(R)$, Theorem 1.1 is a specialization of Theorem 4.8.

2. CAT-GROUPS

Recall that a *symmetric categorical group*, or *cat-group* for short, is a groupoid \mathfrak{G} , equipped with a symmetric monoidal structure $+: \mathfrak{G} \times \mathfrak{G} \rightarrow \mathfrak{G}$, such that for each object X , the endofunctor $(-) + X : \mathfrak{G} \rightarrow \mathfrak{G}$ is an equivalence of categories [8]. In particular, one has an object Y and an isomorphism $X + Y \rightarrow 0$, where 0 is the neutral object with respect to the symmetric monoidal structure $+$. If \mathfrak{G} and \mathfrak{H} are cat-groups, a morphism $\alpha : \mathfrak{G} \rightarrow \mathfrak{H}$ is just a symmetric monoidal functor.

Let \mathfrak{G} be a cat-group. The monoidal structure induces an abelian group structure on the set of connected components. This abelian group is denoted by $\pi_0(\mathfrak{G})$. We also have an abelian group $\pi_1(\mathfrak{G})$, which is the group of automorphisms of the neutral object of \mathfrak{G} . Since the functor $(-) + X : \mathfrak{G} \rightarrow \mathfrak{G}$ is an equivalence of categories for every object X , the induced homomorphism $\pi_1(\mathfrak{G}) \rightarrow \text{Aut}_{\mathfrak{G}}(X)$ is an isomorphism. Because of this, we will identify the automorphism group of any object with $\pi_1(\mathfrak{G})$. Recall also that if $\alpha : \mathfrak{G} \rightarrow \mathfrak{H}$ is a morphism of cat-groups, then α is an equivalence if and only if the induced morphisms

$$\pi_i(\mathfrak{G}) \rightarrow \pi_i(\mathfrak{H}), \quad i = 0, 1$$

are isomorphisms.

We also note that if $\alpha : \mathfrak{G} \rightarrow \mathfrak{H}$ is a morphism of cat-groups, then one can define the cat-group $2\text{-Ker}(\alpha)$. Objects of $2\text{-Ker}(\alpha)$ are pairs (X, x) , where X is an object of \mathfrak{G} , while $x : 0 \rightarrow \alpha(X)$ is a morphism in \mathfrak{H} . A morphism $(X, x) \rightarrow (Y, y)$ in $2\text{-Ker}(\alpha)$ is a morphism $f : X \rightarrow Y$ in \mathfrak{G} , such that $y = \alpha(f)x$. It is also well-known ([3, p. 84], [8]) that there is an exact sequences of abelian groups

$$(1) \quad 0 \rightarrow \pi_1(2\text{-Ker}(\alpha)) \rightarrow \pi_1(\mathfrak{G}) \rightarrow \pi_1(\mathfrak{H}) \rightarrow \pi_0(2\text{-Ker}(\alpha)) \rightarrow \pi_0(\mathfrak{G}) \rightarrow \pi_0(\mathfrak{H}).$$

Recall the definition of an exact sequence of cat-groups [8]. A diagram

$$\begin{array}{ccccc} & & 0 & & \\ & \searrow & \uparrow \kappa & \swarrow & \\ \mathfrak{G} & \xrightarrow{\alpha} & \mathfrak{H} & \xrightarrow{\beta} & \mathfrak{K} \end{array}$$

is called *exact* at \mathfrak{H} , provided the induced functor $\gamma : \mathfrak{G} \rightarrow 2\text{-Ker}(\beta)$ is essentially surjective. More precisely,

$$\gamma(X) = (\alpha(X), \kappa(X) : \beta\alpha(X) \rightarrow 0).$$

It follows that one has an exact sequence of abelian groups

$$\pi_0(\mathfrak{G}) \rightarrow \pi_0(\mathfrak{H}) \rightarrow \pi_0(\mathfrak{K}).$$

If we are given a morphism $\alpha : G \rightarrow H$ of abelian groups, then we can make a cat-group \mathfrak{G}_α whose objects are the elements of H , and for $h_1, h_2 \in H$, we have

$$\text{Hom}(h_1, h_2) = \{g \in G \mid h_2 + \alpha(g) = h_1\}.$$

The monoidal structure is induced by the additive group structure on G and H . We have $\pi_0(\mathfrak{G}_\alpha) = \text{Coker}(\alpha)$ and $\pi_1(\mathfrak{G}_\alpha) = \text{Ker}(\alpha)$.

Let $\alpha : G_0 \rightarrow G_1$ and $\beta : H_0 \rightarrow H_1$ be morphism of abelian groups and \mathfrak{G}_α and \mathfrak{G}_β their associated cat-groups. Observe that any commutative diagram of abelian groups and group homomorphisms

$$\begin{array}{ccc} G_0 & \longrightarrow & H_0 \\ \alpha \downarrow & & \downarrow \beta \\ G_1 & \longrightarrow & H_1 \end{array}$$

gives rise to a morphism of the abelian cat-groups $\mathfrak{G}_\alpha \rightarrow \mathfrak{G}_\beta$. We denote by \mathbf{Pb} the pullback of the diagram

$$\begin{array}{ccc} & H_0 & \\ & \downarrow \beta & \\ G_1 & \longrightarrow & H_1 \end{array}$$

The following result is well known:

Proposition 2.1. *Let \mathfrak{G}_α and \mathfrak{G}_β be as above. We have an equivalence of cat-groups*

$$2\text{-Ker}(\mathfrak{G}_\alpha \rightarrow \mathfrak{G}_\beta) \cong \mathfrak{G}_i,$$

where \mathfrak{G}_i is the abelian cat-group associated to the morphism $i : G_0 \rightarrow \mathbf{Pb}$.

Corollary 2.2. *Let $\alpha : G \rightarrow H$ be a homomorphism of abelian groups and denote the associated cat-groups of $G \rightarrow 0$ and $H \rightarrow 0$ by \mathfrak{G}_G and \mathfrak{G}_H respectively. There is an equivalence of cat-groups*

$$2\text{-Ker}(\mathfrak{G}_G \rightarrow \mathfrak{G}_H) \xrightarrow[\sim]{\alpha_*} \mathfrak{G}_\alpha.$$

3. FREE J-GALOIS ALGEBRAS

3.1. The cat-group $\mathfrak{Qu}_f^{pq}(R)$. Let R be a commutative ring and p and q two elements of R such that $pq + 2 = 0$. These elements will be fixed during this section. Of special interest is the case $p = -2, q = 1$.

Objects of the groupoid $\mathfrak{Qu}_f^{pq}(R)$ are pairs $[a, b]$, where $a, b \in R$ and $a^2 + p^2b \in R^*$. Morphisms $[c, d] \rightarrow [a, b]$ are pairs (u, r) , such that $r \in R, u \in R^*$, and the following relations hold:

$$(2) \quad c = au - pr \quad \text{and} \quad d = u^2b - qrua - r^2.$$

The composition of morphisms is defined by

$$(v, s) \circ (u, r) = (vu, rv + s).$$

The morphism $(1, 0) : [a, b] \rightarrow [a, b]$ is the identity morphism of $[a, b]$. We define the functor

$$\star : \mathfrak{Qu}_f^{pq}(R) \times \mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{Qu}_f^{pq}(R)$$

as follows: On objects we have

$$[a_1, b_1] \star [a_2, b_2] = [a_1a_2, a_1^2b_2 + a_2^2b_1 + p^2b_1b_2],$$

where we write $[a_1, b_1] \star [a_2, b_2]$ instead of $\star([a_1, b_1], [a_2, b_2])$, and on morphisms \star is given by

$$(u_1, r_1) \star (u_2, r_2) = (u_1u_2, -pr_1r_2 + r_1u_2a_2 + u_1a_1r_2).$$

One checks that \star defines a symmetric monoidal structure on $\mathfrak{Qu}_f^{pq}(R)$. The neutral object is $[1, 0]$. Since the pair $(a^2 + p^2b, pb)$ defines a morphism $[a, b] \star [a, b] \rightarrow [1, 0]$, the symmetric monoidal groupoid $\mathfrak{Qu}_f^{pq}(R)$ is in fact a cat-group. Consider the set

$$\mathbb{Z}_{pq}(R) = \{r \in R \mid r^2 = qr\},$$

which is considered as an abelian group via the operation $r +_1 s = r + s + prs$. It is clear that the map $r \mapsto (1 + pr, r)$ yields an isomorphism of groups

$$\mathbb{Z}_{pq}(R) \xrightarrow{\sim} \pi_1(\mathfrak{Qu}_f^{pq}(R)).$$

We let $\mathbf{Qu}_f^{pq}(R)$ be the group of isomorphism classes of $\mathfrak{Qu}_f^{pq}(R)$, that is $\mathbf{Qu}_f^{pq}(R) = \pi_0(\mathfrak{Qu}_f^{pq}(R))$.

Observe that if $p = -2$ and $q = 1$, the above relations are exactly the same as in [4, pp. 29-30]. Hence, $\mathbf{Qu}_f^{-2,1}(R)$ is the same as the *free quadratic group* introduced in [4, p. 31], where it is denoted by $\mathbf{Qu}_f(R)$. Recall that the group $\mathbf{Qu}_f(R)$ is the group of isomorphism classes of free separable R -algebras of rank two [4, Ch. 3A]. We will see in Proposition 4.1 that the groups $\mathbf{Qu}_f^{pq}(R)$ have a similar interpretation for all (p, q) . See [4] for an extensive study of $\mathbf{Qu}_f(R)$. The group $\mathbb{Z}_{-2,1}(R)$ is the group of idempotents of R and it appears in many places, see for example [4, p. 202], where it is denoted by $\mathbb{Z}_2(R)$.

Proposition 3.1 (An equivalence of categories). *Let (p, q) be a pair of elements in R such that $pq + 2 = 0$. For any invertible element $t \in R^*$, there is an equivalence of categories*

$$t_* : \mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{Qu}_f^{pt, t^{-1}q}(R).$$

On objects, the functor t_* is given by

$$t_*([a, b]) = [at, b],$$

while on morphism it is given by $t_*(u, r) = (u, r)$.

3.2. The Cat-group $\mathfrak{G}(R)$ and the morphism $\alpha_f : \mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{G}(R)$. Consider the homomorphism of abelian groups

$$R^* \xrightarrow{sq} R^*, \quad sq(r) = r^2.$$

Denote its associated cat-group by $\mathfrak{G}(R)$. We have

$$\pi_0(\mathfrak{G}(R)) = \mathcal{U}_2(R) \quad \text{and} \quad \pi_1(\mathfrak{G}(R)) = \mu_2(R),$$

where

$$\mathcal{U}_2(R) = R^*/(R^*)^2 \quad \text{and} \quad \mu_2(R) = \{r \in R \mid r^2 = 1\}.$$

Define the morphism of categorical groups

$$\alpha_f : \mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{G}(R)$$

as follows: For an object $[a, b]$ of $\mathfrak{Qu}_f^{pq}(R)$ one puts

$$\alpha_f([a, b]) = a^2 + p^2b.$$

If $(u, r) : [c, d] \rightarrow [a, b]$ is a morphism in $\mathfrak{Qu}_f(R)$, then we have

$$c^2 + p^2d = (au - pr)^2 + p^2(u^2b - qrua - r^2) = u^2(a^2 + p^2b)$$

thanks to equalities in (2). Thus, u can be considered as a morphism $c^2 + 4d \rightarrow a^2 + 4b$ in $\mathfrak{G}(R)$ and we put

$$\alpha_f(u, r) = u : \alpha([c, d]) \rightarrow \alpha([a, b]).$$

The morphism of cat-groups $\alpha_f : \mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{G}(R)$ induces the homomorphisms of abelian groups

$$\mathbb{Z}_{pq}(R) = \pi_1(\mathfrak{Qu}_f(R)) \rightarrow \pi_1(\mathfrak{G}(R)) = \mu_2(R)$$

and

$$\mathfrak{Qu}_f^{pq}(R) \rightarrow \mathcal{U}_2(R).$$

The first homomorphism is given by $a \mapsto 1 + pa$. It is well known that for $p = -2, q = 1$ the second homomorphism fits in the exact sequence (see [4, (3.6) on p.32])

$$(3) \quad \mathfrak{Qu}_f(R) \rightarrow \mathcal{U}_2(R) \rightarrow \mathcal{U}_2(R/4R).$$

We wish to extend this sequence on the left hand side (for arbitrary (p, q)), as well as lift it to the level of cat-groups. This will yield analogous exact sequences after stackification. Observe that the obvious candidate

$$\mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{G}(R) \rightarrow \mathfrak{G}(R/p^2R)$$

does not work, as the composite functor $\mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{G}(R/p^2R)$ is not the trivial one, not even when $p = -2, q = 1$. As such, we have to modify the last cat-group.

3.3. The Cat-group $\mathfrak{G}^{pq}(R)$ and the morphism $\beta_f : \mathfrak{G}(R) \rightarrow \mathfrak{G}^{pq}(R)$. We will need the following easy and well-known fact.

Lemma 3.2. *Let R be a commutative ring and $r \in (R/pR)^*$. If $\tilde{r} \in R/p^2R$ is a lifting of r , then $\tilde{r} \in (R/p^2R)^*$. Moreover, there is a well-defined homomorphism*

$$Sq : (R/pR)^* \rightarrow (R/p^2R)^*$$

given by $Sq(r) = \tilde{r}^2$.

Proof. If r is invertible and $s = r^{-1}$ in R/pR , then $\tilde{r}\tilde{s} = 1 + px$ for some $x \in R/p^2R$. Here \tilde{s} is a lifting of s in R/p^2R and we obtain $\tilde{r}\tilde{s}(1 - px) = 1$. Hence, \tilde{r} is invertible. To show the last assertion, observe that for any $x \in R/p^2R$, one has $(\tilde{r} + px)^2 = \tilde{r}^2 + 2prx = \tilde{r}^2$. This is because $2 = -pq$ and $p^2 = 0$ in R/p^2 . \square

Let $\mathfrak{G}^{pq}(R)$ be the cat-group corresponding to the homomorphism $Sq : (R/pR)^* \rightarrow (R/p^2R)^*$.

Lemma 3.3. *We have*

$$\pi_0(\mathfrak{G}^{pq}(R)) = \mathcal{U}_2(R/p^2R)$$

and

$$\pi_1(\mathfrak{G}^{pq}(R)) = \text{Ker}((R/pR)^* \xrightarrow{Sq} (R/p^2R)^*) \cong \text{Im}(\mu_2(R/p^2R) \rightarrow \mu_2(R/pR)).$$

Proof. To see the first isomorphism, it suffices to note that $\text{Im}(Sq) = \text{Im}((R/p^2R)^* \xrightarrow{sq} (R/p^2R)^*)$. The second statement is obvious. \square

Since the following diagram of abelian groups

$$\begin{array}{ccc} R^* & \longrightarrow & (R/pR)^* \\ sq \downarrow & & \downarrow Sq \\ R^* & \longrightarrow & (R/p^2R)^* \end{array}$$

commutes, it gives rise to a morphism of categorical groups

$$\beta_f : \mathfrak{G}(R) \rightarrow \mathfrak{G}^{pq}(R).$$

3.4. The natural transformation $\delta_f : \beta_f \alpha_f \rightarrow 1$. Take an object $[a, b]$ in $\mathfrak{Qu}_f(R)$. Since $a^2 + p^2b \in R^*$, the element $a(\text{mod } pR)$ is invertible in R/pR . As such, it can be considered as a morphism $a^2(\text{mod } p^2R) \rightarrow 1$ in $\mathfrak{G}^{pq}(R)$. We denote this map by $\delta_f([a, b])$ and obtain $\delta_f([a, b]) : (\beta_f \circ \alpha_f)([a, b]) \rightarrow 1$. Moreover, if $(u, r) : [c, d] \rightarrow [a, b]$ is a morphism of $\mathfrak{Qu}_f^{pq}(R)$, one has $c = ua(\text{mod } pR)$, thanks to the equations in (2) on page 3. This means that the following diagram

$$\begin{array}{ccc} c^2(\text{mod } p^2R) & \xrightarrow{\delta_f([c, d])} & 1 \\ u(\text{mod } pR) \downarrow & \nearrow \delta_f([a, b]) & \\ a^2(\text{mod } p^2R) & & \end{array}$$

commutes in $\mathfrak{G}^{pq}(R)$. Thus, $\delta_f : \beta_f \alpha_f \rightarrow 1$ is a natural transformation from $\beta_f \circ \alpha_f$ to the trivial functor.

3.5. $\mathfrak{Qu}_f^{pq}(R)$ as a 2-kernel. We can now formulate the main result of this section.

Theorem 3.4. *i) The sequence of cat-groups*

$$\begin{array}{ccccc} & & 1 & & \\ & & \delta_f \Uparrow & & \\ \mathfrak{Qu}_f^{pq}(R) & \xrightarrow{\alpha_f} & \mathfrak{G}(R) & \xrightarrow{\beta_f} & \mathfrak{G}^{pq}(R) \end{array}$$

is exact at $\mathfrak{G}(R)$, that is the induced functor

$$\gamma_f : \mathfrak{Qu}_f^{pq}(R) \rightarrow 2\text{-Ker}(\beta_f)$$

is essentially surjective.

ii) If p is not a zero-divisor in R , then γ_f is an equivalence of cat-groups.

Proof. i) According to Proposition 2.1, the cat-group $2\text{-Ker}(\mathfrak{G}(R) \rightarrow \mathfrak{G}^{pq}(R))$ is equivalent to the cat-group \mathfrak{G}_h associated to the following homomorphism of abelian groups:

$$R^* \xrightarrow{h} \{(x, s) | x \in R^*, s \in (R/pR)^*, x \equiv \tilde{s}^2 \pmod{p^2 R}\}.$$

Here $\tilde{s} \in R/p^2 R$ is a lifting of s and

$$h(u) = (u^2, u \pmod{pR}).$$

Hence, the induced functor

$$\gamma : \mathfrak{Qu}_f(R) \rightarrow \mathfrak{G}_h$$

is given by

$$\begin{aligned} \gamma_f([a, b]) &= (a^2 + p^2 b, a \pmod{pR}) \quad (\text{on objects}) \\ \gamma_f(u, r) &= u \quad (\text{on morphisms}). \end{aligned}$$

Take an object (x, s) in \mathfrak{G}_h . By assumption $x \in R^*$ and there are elements $a, b \in R$ such that $x = a^2 + p^2 b$ and $s = a \pmod{pR}$. Thus $\gamma_f([a, b]) = (x, s)$, and so γ_f is surjective on objects.

ii) Thanks to part i), we only need to show that the functor γ_f is full and faithful. Take two objects $[a, b]$ and $[c, d]$ in $\mathfrak{Qu}_f^{pq}(R)$ and let (u, r) and (u', r') be two morphisms $[c, d] \rightarrow [a, b]$. In particular, $c = ua - pr = u'a - pr'$. If $\gamma_f(u, r) = \gamma_f(u', r')$ then $u = u'$, and so $pr = pr'$. Thus $r = r'$, implying that γ_f is faithful. Take a morphism $u : \gamma_f([a, b]) \rightarrow \gamma_f([c, d])$ in \mathfrak{G}_h . By definition, $u \in R^*$ and the following two conditions hold:

$$c^2 + p^2 d = u^2(a^2 + p^2 b) \quad \text{and} \quad c \equiv ua \pmod{pR}.$$

The last condition implies that there exist an element $r \in R$ such that $c = ua + pr$. We have

$$p^2 d = -c^2 + u^2(a^2 + p^2 b) = -(ua + pr)^2 + u^2(a^2 + p^2 b) = p^2(u^2 b - qu^2 a - r^2).$$

Since p is not a zero-divisor in R , we see that $d = u^2 b - qu^2 a - r^2$. This, together with the equality $c = ua + pr$, shows that the pair (u, r) is a morphism $[c, d] \rightarrow [a, b]$ in $\mathfrak{Qu}_f(R)$, implying that γ_f is full. \square

Corollary 3.5. i) For any commutative ring R , one has an exact sequence of abelian groups

$$\mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{U}_2(R) \rightarrow \mathfrak{U}_2(R/p^2 R).$$

ii) If p is not a zero divisor in R , one has an exact sequence of abelian groups

$$0 \rightarrow \mathbb{Z}_{pq}(R) \rightarrow \mu_2(R) \rightarrow \text{Im}(\mu_2(R/p^2 R) \rightarrow \mu_2(R/pR)) \rightarrow \mathfrak{Qu}_f(R) \rightarrow \mathfrak{U}_2(R) \rightarrow \mathfrak{U}_2(R/p^2 R).$$

iii) For any commutative ring R , the functor $\mathfrak{Qu}_f^{1,-2}(R) \rightarrow \mathfrak{G}(R)$ is an equivalence of cat-groups. In particular, $\mathfrak{Qu}_f^{1,-2}(R) \cong \mathfrak{U}_2(R)$.

Proof. i) By applying π_0 to the exact sequence of cat-groups constructed in Theorem 3.4 i), one obtains the exact sequence i). Similarly, exact sequence ii) is a specialization of the above, thanks to Theorem 3.4 ii). If $p = 1$, p is not a zero-divisor and as such we can use Theorem 3.4 ii). The result now follows since $\mathfrak{G}^{1,-2}(R)$ is the trivial cat-group. \square

Remarks i) The exact sequence in Corollary 3.5 i) in the case $p = -2, q = 1$ is well-known (see the statement [4, (3.6) on p.32])). The second exacts sequence however is new, even in the case $p = -2, q = 1$.

ii) If 2 is invertible in R , the categories $\mathfrak{Qu}_f^{-2,1}(R)$ and $\mathfrak{Qu}_f^{1,-2}(R)$ are equivalent (see Proposition 3.1). In this case we recover the well-known isomorphism $\mathfrak{Qu}_f^{-2,1}(R) \cong \mathfrak{U}_2(R)$ see [4, Statement (3.4) i). on p.32].

3.6. An exact sequence. In this section we generalize the result [4, Exercises 6-10, p.41] to arbitrary $\text{Qu}^{pq}(R)$. Define the set

$$\mathcal{V}_1(R) = \{r \in R \mid 1 + pr \in R^*\}$$

and equip it with the operation $+_1$ by declaring

$$r +_1 s := r + s + prs.$$

One easily sees that under this operation $\mathcal{V}_1(R)$ is an abelian group (0 is also the zero with respect to $+_1$). We also need the following set

$$\mathcal{V}_2(R) = \{x \in R \mid 1 + p^2x \in R^*\},$$

which is also an abelian group under the operation $+_2$, where

$$x +_2 y := x + y + p^2xy.$$

It is straightforward to check that the map

$$\zeta : \mathcal{V}_1(R) \rightarrow \mathcal{V}_2(R), \quad \zeta(r) = r^2 - qr$$

is a group homomorphism and as such defines a cat-group, which we denote by $\mathfrak{V}^{pq}(R)$. We have

$$\pi_1(\mathfrak{V}^{pq}(R)) = \{r \in R \mid r^2 = qr \text{ and } 1 + pr \in R^*\},$$

whose group structure agrees with $+_1$. We also set

$$\mathbf{V}^{pq}(R) = \pi_0(\mathfrak{V}^{pq}(R)).$$

In the case when $p = -2$ and $q = 1$, this group is the same group as one defined in [4, Exercise 6, p.41]. We construct the symmetric monoidal functor

$$\rho : \mathfrak{V}^{pq}(R) \rightarrow \mathfrak{Qu}_f^{pq}(R)$$

as follows: On objects it is given by $\rho(x) = [1, x]$. If r is a morphism from y to x in $\mathfrak{V}^{pq}(R)$ (that is, $y = x + (-qr + r^2)(1 + p^2x)$), then $\rho(r) = (1 + pr, r)$, which is considered as a morphism $[1, y] \rightarrow [1, x]$ in $\mathfrak{Qu}_f^{pq}(R)$.

We also need a cat-group $\mathfrak{S}^{p,q}(R)$. The objects of $\mathfrak{S}^{p,q}(R)$ are elements $a \in R$ for which there exist $b \in R$ such that $a^2 + p^2b \in R^*$. Let a and c be objects of $\mathfrak{S}^{p,q}(R)$. A morphism $c \rightarrow a$ is an element $u \in R^*$, for which there exist an element $r \in R$, such that $c = au - pr$. The composition of morphisms and the symmetric monoidal structure is induced by the multiplication in R . One sets

$$\mathbf{S}^{p,q}(R) := \pi_0(\mathfrak{S}^{p,q}(R)).$$

Define a symmetric monoidal functor $\omega : \mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{S}^{p,q}(R)$ as follows: On objects we set $\omega([a, b]) = a$. If $(u, r) : [c, d] \rightarrow [a, b]$ is a morphism of $\mathfrak{Qu}_f^{pq}(R)$, we set $\omega(u, r) = u$.

As already mentioned, the following result is well-known when $p = -2$ and $q = 1$ [4, Exercises 9 and 10, p. 41].

Proposition 3.6. *i) One has a short exact sequence of abelian groups*

$$0 \rightarrow \mathbf{V}^{pq}(R) \xrightarrow{\rho_*} \mathbf{Qu}_f^{pq}(R) \xrightarrow{\omega_*} \mathbf{S}^{p,q}(R) \rightarrow 0,$$

where ρ_* and ω_* are induced by the functors ρ and ω .

ii) If R is a local ring, then $\mathbf{S}^{p,q}(R) = 0$.

iii) If $p \in \text{Rad}(R)$, then $\mathbf{S}^{p,q}(R) = 0$. Here, $\text{Rad}(R)$ is the intersection of all maximal ideals of R . In particular, if $p = 0$, then

$$\mathbf{Qu}_f^{0q}(R) = R/R_0, \quad \text{where} \quad R_0 = \{r^2 + qr \mid r \in R\} \subset R.$$

Proof. i) Let us show that ω_* is an epimorphism. Take an object a of $\mathfrak{S}^{p,q}(R)$. By definition, there exist $b \in R$ such that $a^2 + p^2b \in R^*$. Thus, $[a, b] \in \mathfrak{Qu}_f^{pq}(R)$ and $\omega([a, b]) = a$. To see that $\omega_* \circ \rho_* = 0$, take an object $x \in \mathfrak{V}^{pq}(R)$. We have $1 + p^2x \in R^*$, and hence

$$\omega \circ \rho(x) = \omega([1, x]) = 1.$$

Next we will show exactness at $\mathbf{Qu}_f^{pq}(R)$. Take an object $[a, b]$ of $\mathbf{Qu}_f^{pq}(R)$ such that $\omega_*([a, b]) = 0$. This means that there exist $u \in R^*$ and $r \in R$ such that $1 = au - pr$. We set $d = u^2b - qrua - r^2$. Then (u, r) is a morphism $(1, d) \rightarrow (a, b)$. Thus, the class of $[a, b]$ in $\mathbf{Q}_f^{pq}(R)$ equals the class of $[1, d] = \rho(d)$ and exactness at $\mathbf{Qu}_f^{pq}(R)$ follows. It remains to show that ρ_* is a monomorphism. Assume $x \in R$ is an element satisfying $1 + p^2x \in R^*$ for which there exists a morphism $[1, 0] \rightarrow [1, x]$ in $\mathbf{Qu}_f^{pq}(R)$. There exist $u \in R^*$ and $r \in R$, such that $1 = u - pr$ and $0 = u^2x - qru - r^2$. It follows that $u = 1 + pr \in R^*$ and $0 = (1 + pr)^2x - qr(1 + pr) - r^2$. The last equation is equivalent to $0 = x + (r^2 - rq)(1 + p^2x)$, or $0 = x + {}_{+2}\zeta(r)$. So r defines a morphism from $0 \rightarrow x$ in $\mathfrak{V}^{pq}(R)$. As such, the class of x is zero in $\mathfrak{V}^{pq}(R)$, proving i).

ii) Assume R is a local ring with maximal ideal \mathfrak{m} . Take an object a of $\mathfrak{S}^{pq}(R)$. We have $a^2 + p^2b = v \in R^*$ for some $b \in R$. If $p \in \mathfrak{m}$, then $v^{-1}a^2 = 1 - p^2bv^{-1} \notin \mathfrak{m}$, showing that $v^{-1}a^2$ is invertible. This implies that a is invertible and a^{-1} defines a morphism $1 \rightarrow a$ in $\mathfrak{S}^{pq}(R)$. Therefore the class of a is zero in $\mathfrak{S}^{pq}(R)$. If $p \notin \mathfrak{m}$, p is invertible in R . If a is invertible, we the same argument works as before, so assume $a \in \mathfrak{m}$. Then $1 + a$ is invertible in R . Since

$$a = 1 \cdot (1 + a) - p \frac{1}{p},$$

we see that the pair $(1 + a, \frac{1}{p})$ defines a morphism $a \rightarrow 1$ in $\mathfrak{S}^{pq}(R)$. Hence, the class of a is zero in $\mathfrak{S}^{pq}(R)$, implying that $\mathfrak{S}^{pq}(R) = 0$.

iii) Take an object a of $\mathfrak{S}^{pq}(R)$, that is we have $a^2 + p^2b = v \in R^*$ for some $b \in R$. Thus, $v^{-1}a^2 = 1 - p^2bv^{-1}$ and by Nakayama $1 + \text{Rad}(R) \subset R^*$. Hence, a is invertible and a^{-1} defines a morphism $1 \rightarrow a$ in $\mathfrak{S}^{pq}(R)$, so the class of a is zero in $\mathfrak{S}^{pq}(R)$ and $\mathfrak{S}^{pq}(R) = 0$. \square

4. PROJECTIVE J-GALOIS ALGEBRAS

4.1. Remarks on stacks. We will assume that the reader is familiar with the theory of stacks [6], which are the 2-categorical analogues of sheaves. By definition, a fibered category is nothing other than a contravariant pseudofunctor. It is additionally a stack if some gluing condition holds [6]. One easily observes that if $\alpha : \mathcal{S}_1 \rightarrow \mathcal{S}_2$ is a morphism of stacks, then $2\text{-Ker}(\alpha)$ is also a stack. It is well-known [6] that for any fibered category \mathcal{A} , there exists a stack \mathcal{A}^+ called the stackification of \mathcal{A} . This construction preserves 2-kernels. Recall also that if \mathcal{S} is a stack of cat-groups, then $\pi_1(\mathcal{S})$ is a sheaf but $\pi_0(\mathcal{S})$ need not be a sheaf in general.

The underlying site which we will work with through out this paper is the Zariski site of affine schemes. However, we prefer to work with commutative rings instead of affine schemes. Accordingly, a covariant pseudofunctor from commutative rings to the 2-category of cat-groups is called a stack if the corresponding contravariant pseudofunctor on affine schemes is one. It is clear that the assignments $R \mapsto \mathbf{Qu}_f^{pq}(R), \mathfrak{S}(R), \mathfrak{S}^{pq}(R)$ define fibered categories. Indeed, all of these are prestacks in the sense of [6] because π_1 of the corresponding cat-groups are sheaves. This is clear for $\mathbb{Z}_{p,q}$ and μ_2 because they are representable functors. For $\pi_1(\mathfrak{S}^{pq}(R))$ this follows from Lemma 3.3. We will identify the stackifications of these prestacks and then use Theorem 3.4 to obtain an exact sequence in Theorem 4.8. The case $p = -2, q = 1$ yields exactly Theorem 1.1, which involves the well studied ([4], [7]) group $\mathbf{Qu}(R)$.

4.2. The stack \mathbf{Qu}^{pq} . Let p and q be two elements in R such that $pq + 2 = 0$. We let J be a commutative and cocommutative Hopf algebras which is freely generated as an R -module by 1 and x , with

$$x^2 = qx \quad \text{and} \quad \Delta(x) = x \otimes 1 + 1 \otimes x + p \cdot x \otimes x.$$

It is well-known that any Hopf algebra, which is free of rank two as an R -module, is of this form [5, Theorem 1.2]. Recall that a commutative and associative algebra with unit A is called a *J-Galois algebra*, provided A is a faithful, finitely generated, projective R -module, and there is given an algebra homomorphism $\eta : A \rightarrow A \otimes J$ which makes A a right J -comodule. Further, the composition

$$A \otimes A \xrightarrow{id \otimes \eta} A \otimes A \otimes J \xrightarrow{\mu \otimes id} A \otimes J$$

needs to be an isomorphism, where μ is the multiplication in A [5]. The last condition means that the affine scheme $\text{Spec}(A)$ is a torsor over the group scheme $\text{Spec}(J)$. It follows that the rank of A is 2.

Denote by $\mathfrak{Qu}^{pq}(R)$ the cat-group of J -Galois algebras. Morphisms of $\mathfrak{Qu}^{pq}(R)$ are isomorphism of J -Galois algebras. The monoidal structure is induced by the cotensor product of J . We denote the isomorphism classes of the groupoid $\mathfrak{Qu}^{pq}(R)$ by $\text{Qu}^{pq}(R)$ (the same group is denoted by $A(J)$ in [5]).

Let $\mathfrak{F} : \mathfrak{A} \rightarrow \mathfrak{B}$ be a functor and consider $\{B \in \mathfrak{B} \mid \text{there are } A \in \mathfrak{A} \text{ and } \mathfrak{F}(A) \xrightarrow{\sim} B\}$. We call this the *essential image* of \mathfrak{F} .

Proposition 4.1. *i) There is a symmetric monoidal functor*

$$\mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{Qu}^{pq}(R),$$

which sends an objects $[a, b]$ to (A, η) . Here $A = R[t]/(t^2 - aqt - b)$ while the algebra homomorphism $\eta : A \rightarrow A \otimes J$ is given by $\eta(v) = a \cdot 1 \otimes x + v \otimes 1 + p \cdot v \otimes x$, where v denotes the class of t in A . Moreover, if $(u, r) : [c, d] \rightarrow [a, b]$ is a morphism in $\mathfrak{Qu}_f^{pq}(R)$, the corresponding morphism $B = R[s]/(s^2 - cqs - d) \rightarrow A$ is induced by $s \mapsto ut + r$.

ii) The functor $\mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{Qu}^{pq}(R)$ is full and faithful.

iii) The essential image of $\mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{Qu}^{pq}(R)$ consists of J -Galois algebras which are free as R -modules.

Proof. We will prove only part iii) as the rest is straightforward to check. Take a J -Galois algebra A . Thanks to [5, Corollary 2.5], the submodule spanned by 1 is a free R -module, which is a direct summand of M as an R -module. Hence, $A = R \cdot 1 \oplus V$, where N is projective of rank 1. If A is free as an R -module, then V is a free R -module of rank 1 (see [5, Lemma 1.1]). Denote a generator of V by v . It follows that $v^2 = mv + b$, $\eta(v) = l_0 \cdot 1 \otimes 1 + l_1 \cdot v \otimes 1 + a \cdot 1 \otimes x + l_3 \cdot v \otimes x$ and $\eta(1) = 1 \otimes 1$, for some $a, b, m, l_0, l_1, l_3 \in R$. Since $(\text{Id} \otimes \epsilon) \circ \eta(v) = v$, where $\epsilon : A \rightarrow R$ is the counit of J and $\epsilon(1) = 1, \epsilon(v) = 0$, one obtains $l_0 = 0$ and $l_1 = 1$. Thus

$$(4) \quad \eta(v) = v \otimes 1 + a \cdot 1 \otimes x + l_3 \cdot v \otimes x.$$

The condition $(\text{id} \otimes \Delta) \circ \eta(v) = (\eta \otimes \text{id}) \circ \eta(v)$, implies that

$$(5) \quad al_3 = ap \quad \text{and} \quad l_3^2 = l_3p.$$

Next, consider $1 \otimes 1, 1 \otimes v, v \otimes 1, v \otimes v$ as a base of $A \otimes A$, and $1 \otimes 1, v \otimes 1, 1 \otimes x, v \otimes x$ as a base of $A \otimes J$. One easily computes that the matrix of $(\mu \otimes \text{id}) \circ (\text{id} \otimes \eta) : A \otimes A \rightarrow A \otimes J$ in the chosen bases is

$$\begin{pmatrix} 1 & 0 & 0 & b \\ 0 & 1 & 1 & m \\ 0 & 0 & a & l_3b \\ 0 & 0 & l_3 & a + l_3m \end{pmatrix}$$

Hence, $(\mu \otimes \text{id}) \circ (\text{id} \otimes \eta) : A \otimes A \rightarrow A \otimes J$ is an isomorphism if and only if

$$(6) \quad a^2 + al_3m - l_3^2b \in R^*.$$

It follows from the equations (5) that

$$(l_3 - p)(a^2 + al_3m - l_3^2b) = (l_3 - p)a \cdot a + (l_3 - p)a \cdot l_3m - (l_3 - p)l_3 \cdot l_3b = 0$$

and by the condition (6) that $l_3 = p$. Thus, we have

$$(7) \quad \eta(v) = v \otimes 1 + a \cdot 1 \otimes x + p \cdot v \otimes x \quad \text{and} \quad a^2 + pam - p^2b \in R^*.$$

As, η is an algebra homomorphism, we have

$$m \cdot v \otimes 1 + ma \cdot 1 \otimes x + mp \cdot v \otimes x + b \cdot 1 \otimes 1 = \eta(mv + b) = \eta(v^2) = (v \otimes 1 + a \cdot 1 \otimes x + p \cdot v \otimes x)^2,$$

from which we obtain that

$$am = a^2q, \quad \text{and} \quad mp = -2a.$$

Lastly, we have

$$(m - aq)(a^2 + pam - p^2b) = 0,$$

and thus $m = aq$. It follows that $v^2 = aqv + b$ and $a^2 + pam - p^2b = -(a^2 + p^2b) \in R^*$. Hence, A is in the image of the functor $\mathfrak{Qu}_f^{pq}(R) \rightarrow \mathfrak{Qu}^{pq}(R)$ s. \square

Corollary 4.2. *The stackification of $R \mapsto \mathfrak{Qu}_f^{pq}(R)$ is $R \mapsto \mathfrak{Qu}^{pq}(R)$.*

Proof. The descent theory of projective modules implies that the assignment $R \mapsto \mathfrak{Qu}^{pq}(R)$ is a stack, which, by abuse of notation, we denote by \mathfrak{Qu}^{pq} . Proposition 4.1 shows that the natural morphism $\mathfrak{Qu}_f \rightarrow \mathfrak{Qu}$ is a weak equivalence in the sense of [6, Definition 2.3] and hence the result follows. \square

4.3. The stack \mathfrak{Pic} . Let R be a commutative ring. We let $\mathfrak{Pic}(R)$ be the following cat-group: The Objects of $\mathfrak{Pic}(R)$ are projective R -modules of rank 1, while its morphisms are isomorphisms of R -modules. The tensor product \otimes_R equips $\mathfrak{Pic}(R)$ with the structure of a cat-group. If $f : R \rightarrow S$ is a homomorphism of commutative rings, the functor $f_* : \mathfrak{Pic}(R) \rightarrow \mathfrak{Pic}(S)$, given by $f_*(M) = M \otimes_R S$, is a morphism of cat-groups.

It follows from the descent theory that $R \mapsto \mathfrak{Pic}(R)$ is a stack, which we denote by \mathfrak{Pic} . Actually, it is the stackification of the prestack assigning to R the cat-group corresponding to the homomorphism $R^* \rightarrow \{1\}$ (see [6, Example (ii), p. 11]).

It is well-known that

$$\pi_1(\mathfrak{Pic}(R)) = R^*, \quad \text{and} \quad \pi_0(\mathfrak{Pic}(R)) = \text{Pic}(R).$$

4.4. The stack \mathfrak{Dis} . Objects of the category $\mathfrak{Dis}(R)$ are pairs (M, μ) , where M is a finitely generated projective R -module of rank 1 and μ is a nonsingular, symmetric, bilinear form on M . Morphisms $(M, \mu) \rightarrow (M', \mu')$ are isomorphisms of R -modules $h : M \rightarrow M'$, such that $\mu'(h(x), h(y)) = \mu(x, y)$. Define the symmetric monoidal structure on $\mathfrak{Dis}(R)$ by $(M', \mu') \otimes (M'', \mu'') = (M \otimes M, \mu)$, where

$$\mu(m'_1 \otimes m''_1, m'_2 \otimes m''_2) = \mu'(m'_1, m'_2) \mu''(m''_1, m''_2).$$

The neutral object is (R, μ) , where $\mu(r_1, r_2) = r_1 r_2$.

Lemma 4.3. *One has an equivalence of cat-groups:*

$$\mathfrak{Dis}(R) \cong 2\text{-Ker}(sq_R : \mathfrak{Pic}(R) \rightarrow \mathfrak{Pic}(R)).$$

In particular, \mathfrak{Dis} is a stack, which is the stack associated to the prestack $R \mapsto \mathfrak{G}(R)$.

Proof. Let μ be a nonsingular, bilinear form on a projective module M of rank 1. Then $\mu : M \otimes_R M \rightarrow R$ is an isomorphism, where R is seen as the trivial module, and hence defines an object of $2\text{-Ker}(sq_R : \mathfrak{Pic}(R) \rightarrow \mathfrak{Pic}(R))$. One easily checks that this construction yields an equivalence of categories

$$\mathfrak{Dis}(R) \cong 2\text{-Ker}(sq_R : \mathfrak{Pic}(R) \rightarrow \mathfrak{Pic}(R)).$$

We use Corollary 2.2 to show the last statement. It says that the cat-group $\mathfrak{G}(R)$ is the 2-kernel of the morphism of cat-groups (associated to the vertical arrows), corresponding to the commutative diagram of abelian groups

$$\begin{array}{ccc} R^* & \xrightarrow{sq} & R^* \\ \downarrow & & \downarrow \\ 1 & \longrightarrow & 1. \end{array}$$

We see that the stackification of $R \mapsto \mathfrak{G}(R)$ is the 2-kernel of $sq : \mathfrak{Pic} \rightarrow \mathfrak{Pic}$, which is \mathfrak{Dis} , since stackification preserves 2-kernels. \square

Note that equivalent prestacks give rise to equivalent stackifications and recall the exact sequence (1) on page 2. Denote $\text{Dis}(R) := \pi_0(\mathfrak{Dis}(R))$. We have the following results:

Corollary 4.4. *i) There is an exact sequence ([4, (12.4) on p. 176])*

$$0 \rightarrow \mathbf{U}_2(R) \rightarrow \mathbf{Dis}(R) \rightarrow {}_2\mathbf{Pic}(R) \rightarrow 0.$$

ii) We have an isomorphism of abelian groups

$$\pi_1(\mathbf{Dis}(R)) \cong \mu_2(R) = \{x \in R \mid x^2 = 1\}.$$

iii) Propositions 3.1 and 4.1 imply that one has an equivalence of cat-groups

$$t_*^+ : \mathbf{Qu}^{pq}(R) \rightarrow \mathbf{Qu}^{pt, t^{-1}q}(R).$$

iv) From Corollary 3.5 iii) we immediately get that $\mathbf{Qu}^{1,-2} \cong \mathbf{Dis}$. If 2 is invertible in R , the second of the remark on page 6 yields the equivalence of cat-groups

$$\mathbf{Qu}^{-2,1}(R) \cong \mathbf{Dis}(R).$$

After applying π_0 , we get the classical result ([4, (12.8) on p. 183])

$$\mathbf{Qu}(R) \cong \mathbf{Dis}(R).$$

4.5. The stack \mathbf{Dis}^{pq} . We will need some morphism of stacks. The first one $sq : \mathfrak{Pic} \rightarrow \mathfrak{Pic}$ is given by $sq(M) = M \otimes_R M$, $M \in \mathfrak{Pic}(R)$.

Proposition 4.5. *There is a morphism of cat-groups*

$$Sq : \mathfrak{Pic}(R/p^2R) \rightarrow \mathfrak{Pic}(R/p^2R),$$

for which the following diagram

$$\begin{array}{ccc} \mathfrak{Pic}(R/p^2R) & \xrightarrow{\quad} & \mathfrak{Pic}(R/pR) \\ sq \downarrow & \swarrow Sq & \downarrow sq \\ \mathfrak{Pic}(R/p^2R) & \xrightarrow{\quad} & \mathfrak{Pic}(R/pR) \end{array}$$

commutes up to natural isomorphisms. Here, the horizontal arrows are induced by the obvious ring homomorphism $R/p^2R \rightarrow R/pR$.

Proof. Since the kernel of the ring homomorphism $R/p^2R \rightarrow R/pR$ is a nilpotent ideal, the functor $\mathfrak{Pic}(R/p^2R) \rightarrow \mathfrak{Pic}(R/pR)$ is full, essentially surjective and reflects isomorphisms (see for example [2, Proposition 2.12]). Hence, the result follows from Lemma 4.6 below. \square

Lemma 4.6. *Let $f, g : M \rightarrow N$ be two morphisms in $\mathfrak{Pic}(R/p^2R)$ such that the induced maps $f_*, g_* : M/pM \rightarrow N/pN$ coincide. Then, $sq(f) = sq(g) : sq(M) \rightarrow sq(N)$.*

Proof. This result can be checked locally, so we may assume that $M = N = R/p^2R$. There are $a, b \in R/p^2R$ such that $f(x) = ax$ and $g(x) = bx$ for all $x \in R/p^2R$. By assumption, $b = a + pr$ for some $r \in R/p^2R$. We have

$$sq(g)(xy) = g(x)g(y) = b^2xy = (a + pr)^2xy = a^2xy - p^2qar = a^2xy = f(x)f(y) = sq(f)(xy).$$

\square

We now put

$$\mathbf{Dis}^{pq}(R) = 2\text{-Ker}(Sq : \mathfrak{Pic}(R/pR) \rightarrow \mathfrak{Pic}(R/p^2R)).$$

Since the 2-kernel of a morphism of stacks is again a stack, we see that \mathbf{Dis}^{pq} is the stack associated to the prestack $R \mapsto \mathfrak{Pic}^{pq}(R)$.

Lemma 4.7. *One has natural isomorphisms*

$$\pi_0(\mathbf{Dis}^{pq}(R)) = \mathbf{Dis}(R/p^2R) \quad \text{and} \quad \pi_1(\mathbf{Dis}^{pq}(R)) \cong \text{Ker}(Sq : (R/pR)^* \rightarrow (R/p^2R)^*).$$

Proof. By our construction, we have a diagram of cat-groups

$$\begin{array}{ccc} \mathfrak{Pic}(R/p^2R) & \xrightarrow{sq} & \mathfrak{Pic}(R/p^2R) \\ \downarrow & & \downarrow id \\ \mathfrak{Pic}(R/pR) & \xrightarrow{sq} & \mathfrak{Pic}(R/p^2R) \end{array}$$

which commutes up to a natural isomorphism. We apply the exact sequence (1), p.2 to the horizontal morphisms. It follows from the discussion on [3, p. 88] that one obtains a commutative diagram with exact rows

$$\begin{array}{ccccccccccc} 0 \longrightarrow \mu_2(R/p^2R) \longrightarrow (R/p^2R)^* & \xrightarrow{sq} & (R/p^2R)^* & \longrightarrow & \text{Dis}(R/p^2R) & \longrightarrow & \text{Pic}(R/p^2R) & \xrightarrow{sq} & \text{Pic}(R/p^2R) \\ \downarrow & & \downarrow & & \downarrow id & & \downarrow & & \downarrow id \\ 0 \longrightarrow \pi_1(\mathfrak{Dis}^{pq}(R)) \longrightarrow (R/pR)^* & \xrightarrow{sq} & (R/p^2R)^* & \longrightarrow & \pi_0(\mathfrak{Dis}^{pq}(R)) & \longrightarrow & \text{Pic}(R/pR) & \xrightarrow{sq} & \text{Pic}(R/p^2R). \end{array}$$

This already imply the result for $\pi_1(\mathfrak{Dis}^{pq}(R))$. Since the kernel of $R/p^2R \rightarrow R/pR$ is a nilpotent ideal, the vertical map $\text{Pic}(R/p^2R) \rightarrow \text{Pic}(R/pR)$ is an isomorphism and $(R/p^2R)^* \rightarrow (R/pR)^*$ is an epimorphism ([2, Proposition IX.3.4]). Hence the result is also true for $\pi_0(\mathfrak{Dis}^{pq}(R))$, thanks to the 5-lemma. \square

4.6. The main result. After stackification of the prestacks involved in the diagram described in Theorem 3.4, one obtains the diagram of stacks

$$\begin{array}{ccccc} & & 1 & & \\ & \searrow & \delta \uparrow & \nearrow & \\ \mathfrak{Qu} & \xrightarrow{\alpha} & \mathfrak{Dis} & \xrightarrow{\beta} & \mathfrak{Dis}^{pq}. \end{array}$$

By general properties of stackification, Theorem 3.4 i) implies that the induced functor

$$\gamma : \mathfrak{Qu} \rightarrow 2\text{-Ker}(\beta)$$

is locally essentially surjective.

Assume that p is not a zero-divisor in R . One easily sees that the same property holds for the localization ring R_r , where $r \in R$. It follows that p is not a zero divisor for any of the rings involved in the process of stackification. By Theorem 3.4 ii), the induced morphism

$$\gamma(R) : \mathfrak{Qu}^{pq}(R) \rightarrow 2\text{-Ker}(\mathfrak{Dis}(R)) \xrightarrow{\beta(R)} \mathfrak{Dis}^{pq}(R)$$

is an equivalence of cat-groups. The following is now a specialization of the exact sequence (1):

Theorem 4.8. *If p is not a zero divisor of R , one has an exact sequence of abelian groups*

$$0 \rightarrow \mathbb{Z}_{pq}(R) \rightarrow \mu_2(R) \rightarrow \text{Im}(\mu_2(R/p^2R) \rightarrow \mu_2(R/pR)) \rightarrow \mathfrak{Qu}^{pq}(R) \rightarrow \text{Dis}(R) \rightarrow \text{Dis}(R/p^2R).$$

REFERENCES

- [1] H. BASS. Lectures on topics in algebraic K-theory. Tata Institut of Fundamental Research. Bombay. 1967.
- [2] H. BASS. Algebraic K-theory. Benjamin. N.-Y. 1968.
- [3] P. GABRIEL and M. ZISMAN. Calculus of fractions and homotopy theory. Ergebnisse der Mathematik und ihrer Grenzgebiete. Band 35. Springer Verlag, Berlin. (1967).
- [4] A. J. HAHN. Quadratic algebras, Clifford algebras, and arithmetic Witt groups. Universitext. Springer Verlag, Berlin (1993).
- [5] H.F.KREIMER. Quadratic Hopf algebras and Galois extensions, in Algebrasts' homage: Papers in ring theory and and related topics. Comtemp. Math. v. 13(1982),353-361.
- [6] I. MOERDIJK. Introduction to the language of stacks and gerbes. arXiv: math.AT/0212266.
- [7] C. SMALL. The group of quadratic extensions. J. Pure and Appl. Algebra. 2(1972), 83-105.
- [8] E. M. VITALE. A Picard-Brauer exact sequence of categorical groups. J. Pure and Appl. Algebra. 175(2002), 283-408.

E-mail address: ilia_p@ymail.com